but without the claims) contains no new matter. As required by 37 C.F.R. § 1.121(b)(3)(iii) and § 1.125(b)(2), a Marked Up Version Of The Substitute Specification comparing the original Specification and the Substitute Specification also accompanies this Amendment. In the Marked Up Version, double-underlining indicates added text and bracketing indicates deleted text. Approval and entry of the Substitute Specification (including Abstract) is respectfully requested.

With respect to paragraphs four (4) and five (5) of the Office Action, claims 11 to 23 were rejected under 35 U.S.C. § 112, first paragraph, as being unenabled by the specification. Specifically, in response to the Office Action's rejection, the method of calculating a checksum claimed in claim 11 is discussed in the original Specification (as well as in the above-submitted Substitute Specification) at least at page 2, line 18 to page 3, line 17. Further, in response to the Office Action's rejections, the details of the generating of the authentication token claimed in claims 14 and 17 are discussed in the original Specification (as well as in the above-submitted Substitute Specification) at least at page 7, lines 16-18. (Note that there was a typographical error at line 17 – "s[w]+t[i]" should be "s[w]⊕t[i]" – this error has been corrected in the above-submitted Substitute Specification at page 7, line 23. No new matter has been added.) Further, in response to the Office Action's rejections, the characteristics of the block cipher claimed in claims 18 and 19 are discussed in the original Specification (as well as in the above-submitted Substitute Specification) at least at page 2, line 24 to page 3, line 2. Further, in response to the Office Action's rejection, the calculation of the token claimed in claim 22 is discussed in the original Specification (as well as in the above-submitted Substitute Specification) at least at page 3, lines 10-17. Further, in response to the Office Action's rejection, the details of the coding of signals using strings of the pseudo-random sequence claimed in claims 13 and 16 are discussed in the original Specification (as well as in the above-submitted Substitute Specification) at least at page 2, lines 18 to page 3, line 2, and page 6, line 4 et seq. Accordingly, Applicant respectfully submits that in the citations listed above, as well as throughout the Specification, the features of claims 11, 13, 14, 16 to 19, and 22, are enabled and therefore the rejection of claims 11 to 23 should be withdrawn.

With respect to paragraphs six (6) and seven (7) of the Office Action, claims 11 to 23 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite in light of the specification. The Specification has been amended as respectfully submitted above, thus, Applicant respectfully believes that any indefiniteness has been alleviated by the discussion

above and claims 11 to 23 are now in a condition for allowance. Accordingly, withdrawal of the rejection of claims 11 to 23 is respectfully requested.

It is therefore respectfully submitted that claims 11 to 23 are allowable for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that any objections to the Specification and rejections to claims 11 to 23 have been obviated, and that the Substitute Specification and the claims 11 to 23 are allowable. It is therefore respectfully requested that any objections and rejections be withdrawn, and that the present application issue as early as possible.

If for any reason the Examiner believes that contact with Applicant's attorney would advance the prosecution of this application, he or she is invited to contact the undersigned at the number given below.

Respectfully submitted,

By: Richard L. Mayer
Reg. No. 47084

Dated: August 20, 2002

By: Richard L. Mayer
Richard L. Mayer
(Reg. No. 22,490)

KENYON & KENYON
One Broadway
New York, New York 10004
1 (212) 425-7200

CUSTOMER N0. 26646

#7

[2345/62]

SIGNAL TRANSMISSION PROCESS

FIELD OF THE INVENTION

The present invention relates to a method of transmitting signals [according to the definition of the species of Patent Claim 1.

]between a transmitter and a receiver using keys and cryptographic algorithms.

RELATED TECHNOLOGY

In transmission of signal sequences, authentic transmission of the data or signals [always]plays a major role. For example, one method of achieving this goal is described in ISO/IEC 9797, Information Technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm (JTC1/SC27 1994). Identical secret keys in combination with an encoding algorithm (block cipher, encipherment algorithm) or with a key-dependent single-way function (cryptographic check function) are assigned to the transmitter and the receiver. This can take place, for example, on a card. The transmitter adds a cryptographic check sum (message authentication code) to each signal (datum) depending on the secret key and the cryptographic algorithm (encoding or single-way function). The receiver in turn calculates the check sum and acknowledges the received signals as authentic if the check sum is identical. However, this method has the following disadvantages: to detect a change in sequence of transmitted data, the check sum of a signal is calculated as a function of the check sum of the signals transmitted previously. Even in the case when a check sum is transmitted after each signal, this is still necessary because otherwise a hacker could record pairs of signal check sums and enter them in an altered sequence without being detected. With the [known]available method, this requires the cryptographic algorithm to be executed for each check sum. Since the sequence and selection of signals are not precisely fixed in advance, it [is]can be impossible to calculate the required check sums in advance.

This can lead to problems in a time-critical environment. The cryptographic algorithm can be calculated on a chip card, for example. This [is]may be advantageous when using a chip card that has already been evaluated, [but]because otherwise an additional software implementation of the algorithm must be evaluated again. Communication with the chip card and calculation of the cryptographic algorithm on the card [are]can be very time intensive.

[Therefore, the object]SUMMARY

Example embodiments and/or example methods of the present invention [is]are directed to [create]creating a method of authentic signal and data transmission that will permit calculation of authentication information with a given signal supply and a given maximum number of signals to be transmitted, so that check sums for the signals and/or data transmitted can be calculated quickly and easily from this previously calculated information in the transmission phase.

[The method of achieving this goal according to the present invention is presented in the characterizing part of Patent Claim 1.

Additional embodiments of the object]Example embodiments and/or example methods of the present invention [and methods of achieving this goal are presented in the characterizing parts of Patent Claims 2 through 10]are directed to providing a method for transmitting signals between a transmitter and a receiver, the method including calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, and calculating authentication tokens for the signals as a function of the data, in a communication phase, so as to authenticate both the signals and a transmission sequence of the signals.

By intentionally introducing a preliminary calculation phase and a communication phase into the transmission process, [it is]one may now[possible to] perform the calculation of authentication information before the actual[the] transmission phase, and then during the transmission phase, check sums for the signals transmitted can be

calculated easily and quickly from this information already calculated. [The desired object is]This may be achieved by a method composed of a preliminary calculation phase and a communication phase in which the signals or data are transmitted together with the check sums. In the preliminary calculation phase, first a pseudo-random sequence Z is generated by cryptographic algorithms, e.g., a block cipher in the output feedback mode, from the time-variant parameter (sequence number, time mark and other initialization data). As an example, m = 16, 32 or 64 is assumed for a security parameter m. Then nonintersecting strings z(i) of m bits each from the sequence Z are assigned to the signals s[i], i = 1, 2, ..., n of the signal supply. Additional nonintersecting m-bit strings t[i] are selected from the remaining sequence as the coding of the numbers 1, 2, ... MAX, where MAX is the maximum number of signals to be transmitted.

If transmitter authentication is necessary in the subsequent communication phase, then first the sequence of one pass authentication [is followed]may be performed according to the [publications]reference(s) ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms, (JTC1/SC27 1994) and ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995). The transmitter may transmit[s] the initialization information and the time-variant parameters to the receiver, and it may transmit[s] a number of previously unused bits from Z to the receiver as an authentication token. The receiver in turn may calculate[s] pseudo-random sequence Z and check[s] the received authentication token. The signals received by the receiver during the signal transmission are accepted as authentic if the received authentication token matches the token calculated. In addition, modifications of the method are also possible, as described [in detail in the following specification.

The present invention will now be described in greater detail on the basis of embodiments illustrated in the drawing, which shows:

a) Transmitter authentication:

If transmitter authentication is necessary, first the sequence of one pass authentication is followed according to the [publication]reference ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994), and ISO/IEC 9798-4 Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995). The transmitter transmits the initialization information and the time-variant parameters to the receiver. It transmits as the authentication token a number of previously unused bits from Z to the receiver. The receiver in turn may calculate[s] pseudo-random sequence Z and checks the received authentication token.

b) Signal transmission and authentication:

Let s[k[1]] be the first signal transmitted; then the transmitter transmits T(1): = f(z[k[1]], t[1]), where f is a link between the two values z[k[1]] and t[1] that can be calculated rapidly for authentication of the first signal. One example of f is the bit-by-bit XOR link.

For i = 2, 3, ..., i maximally MAX, let s[k[i]] be the i-th signal transmitted. For authentication of this signal, the transmitter may transmit[s] token T(i): = f(z[k[i]], t[i]). The receiver may perform[s] the same calculations and accepts the received signals as authentic if the authentication token received by the transmitter matches the token calculated.

The sequence of transmitted signals [is]may be guaranteed by the influence of the values t[i].

One variant of signal authentication proceeds as follows: If it is necessary to select authentication token T(i) of the i-th signal s[k[i-1]] as a function of all previously

E2 and S2: The transmitter and receiver here first calculate a random sequence PRS (pseudo-random sequence) of length m* (smax + tmax) bits, where

m: security parameter, namely in this example m: = 32.

smax: Maximum number of different signals (number of elements of the alphabets/signal supply). In the telephone example, this refers to digits 1 through 9 and special symbols such as # and others.

tmax: Maximum number of signals to be authenticated in one pass. In the telephone example this [would]may be the maximum length of a telephone number, the maximum number of digits and special symbols for establishing a connection.

Then nonintersecting strings of m bits of this random sequence PRS [are]may be assigned to m-bit quantities s[1], s[2], ..., s[smax], t[1], t[2], ..., t[tmax], etc.

s[1] = bit 1 through bit m of the PRS

s[2] = bit m+1 through bit 2*m of the PRS

...

s[max] = bit (smax-1)*m+1 through bit smax*m of random sequence PRS

t[1] = bit smax*m+1 through bit (smax+1)*m of random sequence PRS

t[tmax] = bit (smax+tmax-1)*m+1 through bit (smax+tmax)*m of random sequence PRS

[The]An example sequence of operations or steps for the transmitter is described below on the basis of Figure 2.

S3: The transmitter waits for signal w which is to be transmitted authentically; w is interpreted as a natural number between 1, 2, ..., smax in order to keep the mapping w -> s[w] simple.

S4: The transmitter sends the I-th signal w together with authentication token

f(s[w], t[i]). In the telephone example, the token is f(s[w], t[i]) = s[w][+t]⊕t[i], the bit-by-bit XOR[link] of s[w] and t[i].

S5: S3 and S4 [are]may be iterated either until no more signals are to be transmitted authentically or until the maximum number of signals that can be authenticated with this supply of previously calculated random sequence PRS has been reached.

S6: In the telephone example, the transmitter is now waiting for a connection to be established with the receiver.

E3, E4 and E5: As long as new signals with the respective authentication tokens are received, the receiver checks on whether the authentication tokens calculated by it match the received tokens.

E6: If all the tokens match, the received signals are accepted as authentic. In the telephone example, the connection is now established.

E7: If authentication is unsuccessful, no connection is established.

[Abstract]ABSTRACT OF THE DISCLOSURE

A [process]method and/or system for transmitting sequences of signals/data from a transmitter to a receiver and for authenticating the sequences of signals/data may consist[s] of a precalculation phase and of a communication phase in which the signals are transmitted together with the checking sums. In the precalculation phase, a pseudo-random sequence [is]may be first generated by means of a cryptographic algorithm from a time-variable parameter and other initialization data. Non-overlapping sections (z(1) of a sequence (z) having each m bits [are]may be associated to signals (s(i)), wherein i = 1, 2, ... n, of a signal storage. Further non-overlapping m bit sections (t(i)) of the remaining sequence [are]may be selected for coding numbers (1, 2, ... MAX). The transmitter may transmit[s] the initiali[s]zation information and the time-variable parameters to the receiver and the receiver may calculate[s] the pseudo-random sequence (Z) and checks the received authentication token (T). The transmitter may accept[s] the received signals as being authentic when the received authentication tokens match the calculated ones.